

## Práctica-(Tarea)

### Recopilación Pasiva de Información utilizando Google Hacking y Shodan



Alejandro Garcia Burguillos

15/11/2024

# Informe de Google Hacking y Exploración de Shodan

## Parte 1: Google Hacking

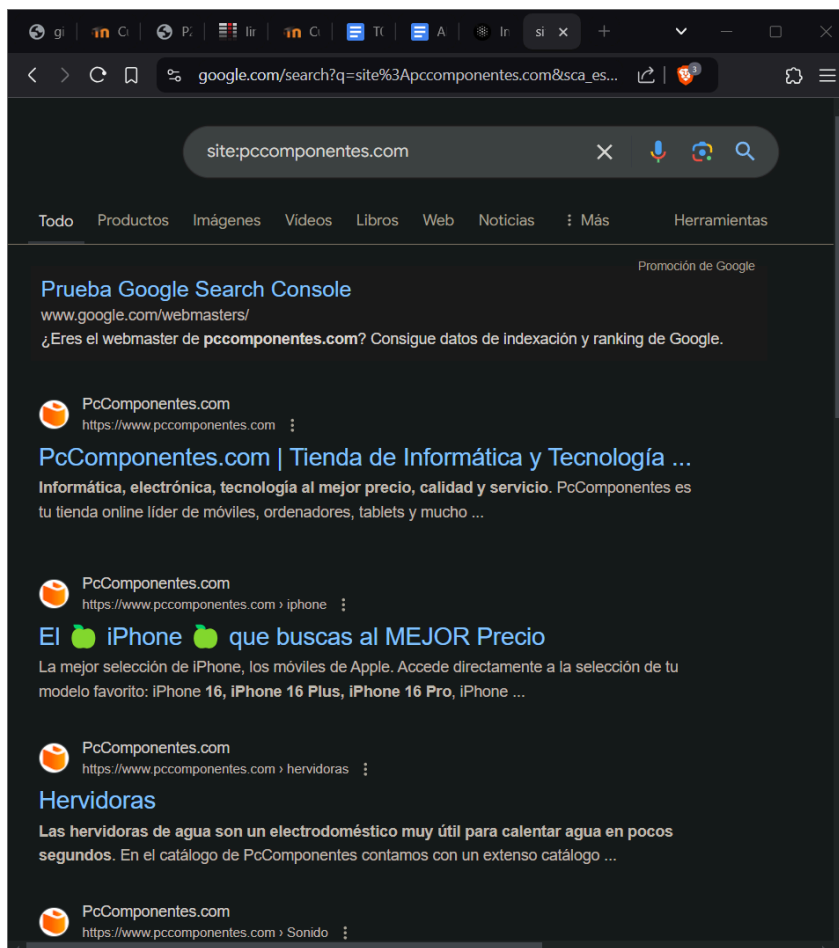
### Organización Seleccionada

Para este ejercicio, he elegido pccomponentes empresa conocida de sobra aquí en España.

### Búsquedas Avanzadas en Google

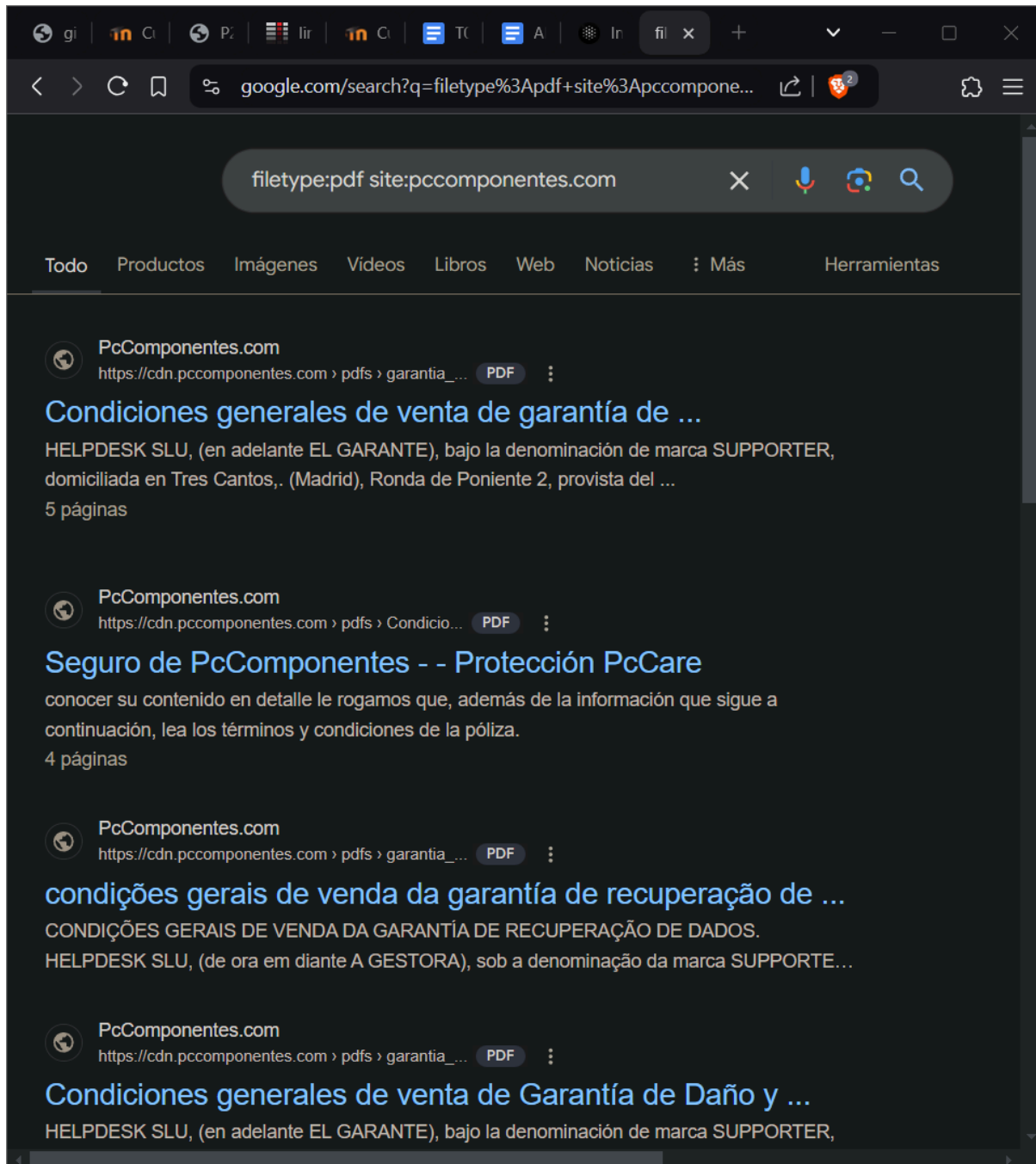
#### 1. Búsqueda: **site:pccomponentes.com**

- Resultados: Listado de páginas indexadas del sitio oficial de la organización.



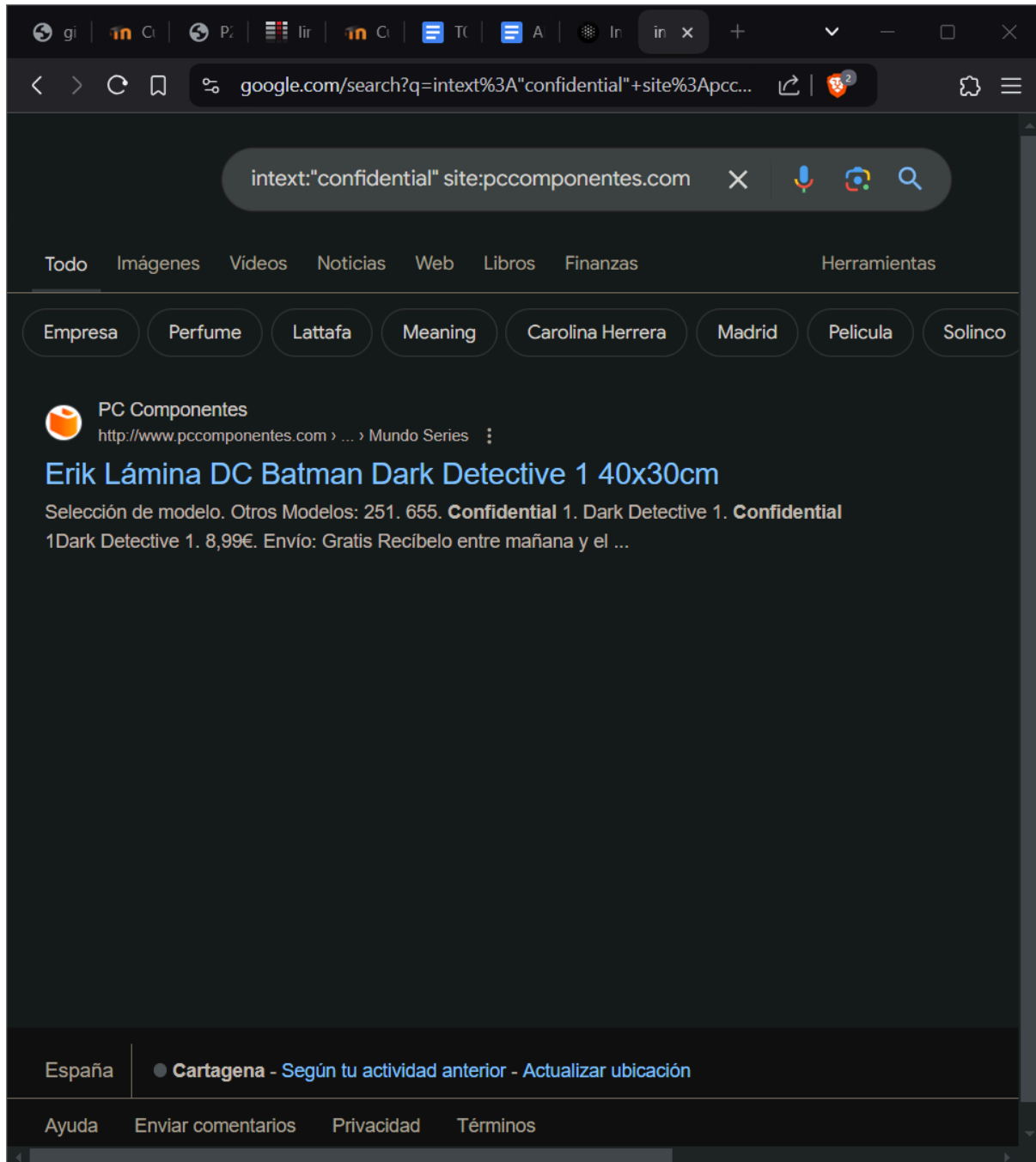
## 2. Búsqueda: filetype:pdf site:pccomponentes.com

- Resultados: Documentos PDF disponibles en el sitio, incluyendo seguro y condiciones del servicio.



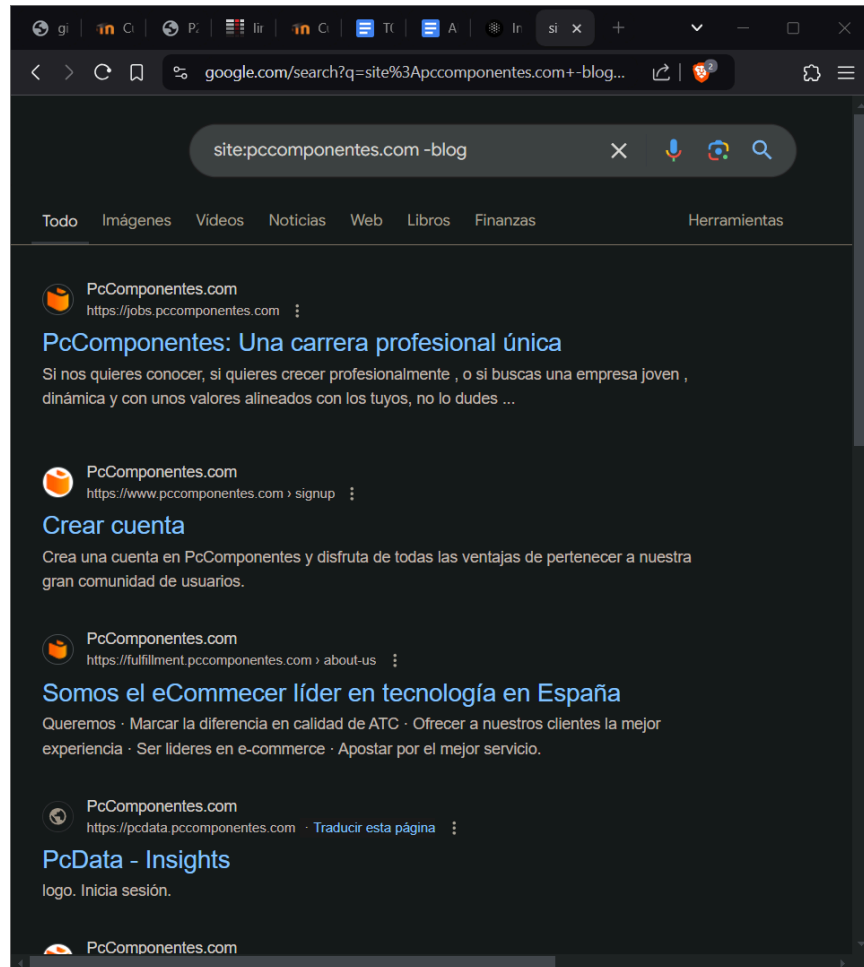
### 3. Búsqueda: **intext:"confidential" site:pccomponentes.com**

- Resultados: Se encuentra una página pero no se encontraron documentos que contengan la palabra "confidential", lo que indica una buena práctica en la gestión de la información sensible.



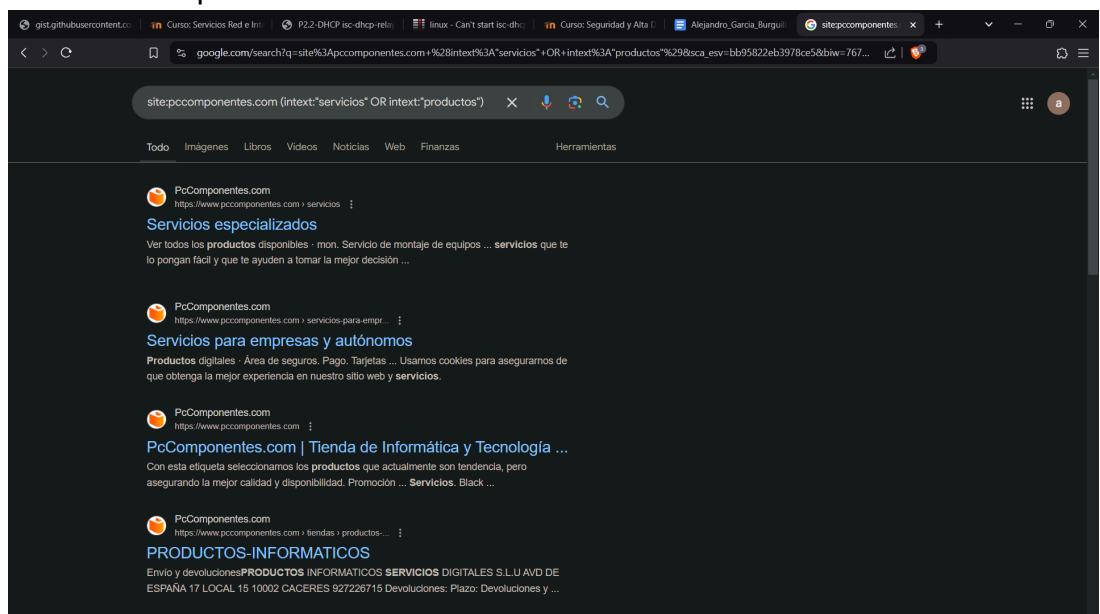
#### 4. Búsqueda: **site:pccomponentes.com -blog**

- Resultados: Listado de páginas del sitio excluyendo la sección del blog.



#### 5. Búsqueda: **site:pccomponentes.com (intext:"servicios" OR intext:"productos")**

- Resultados: Esta búsqueda busca páginas que contengan las palabras "servicios" o "productos" en el texto. Esto puede ayudar a identificar las ofertas específicas.



# Consultas con Google Dorks

Accedemos a [Exploit DB](#).

## 1. Dork: **site:github.com "BEGIN OPENSSSH PRIVATE KEY"**

- Búsqueda: No se encontró nada expuesto por lo menos en las primeras páginas, todo son resolución de problemas sobre el tema.

The image shows two browser windows. The left window displays the Exploit DB 'Google Hacking Database' interface. The search query 'site:github.com "BEGIN OPENSSSH PRIVATE KEY"' is entered in the 'Quick Search' box. Below the search bar, a table lists search results with columns for 'Date Added' and 'Dork'. The right window shows the Google search results for the same query. The search bar contains the query, and the results list several GitHub issues and gists related to OpenSSH private key formats.

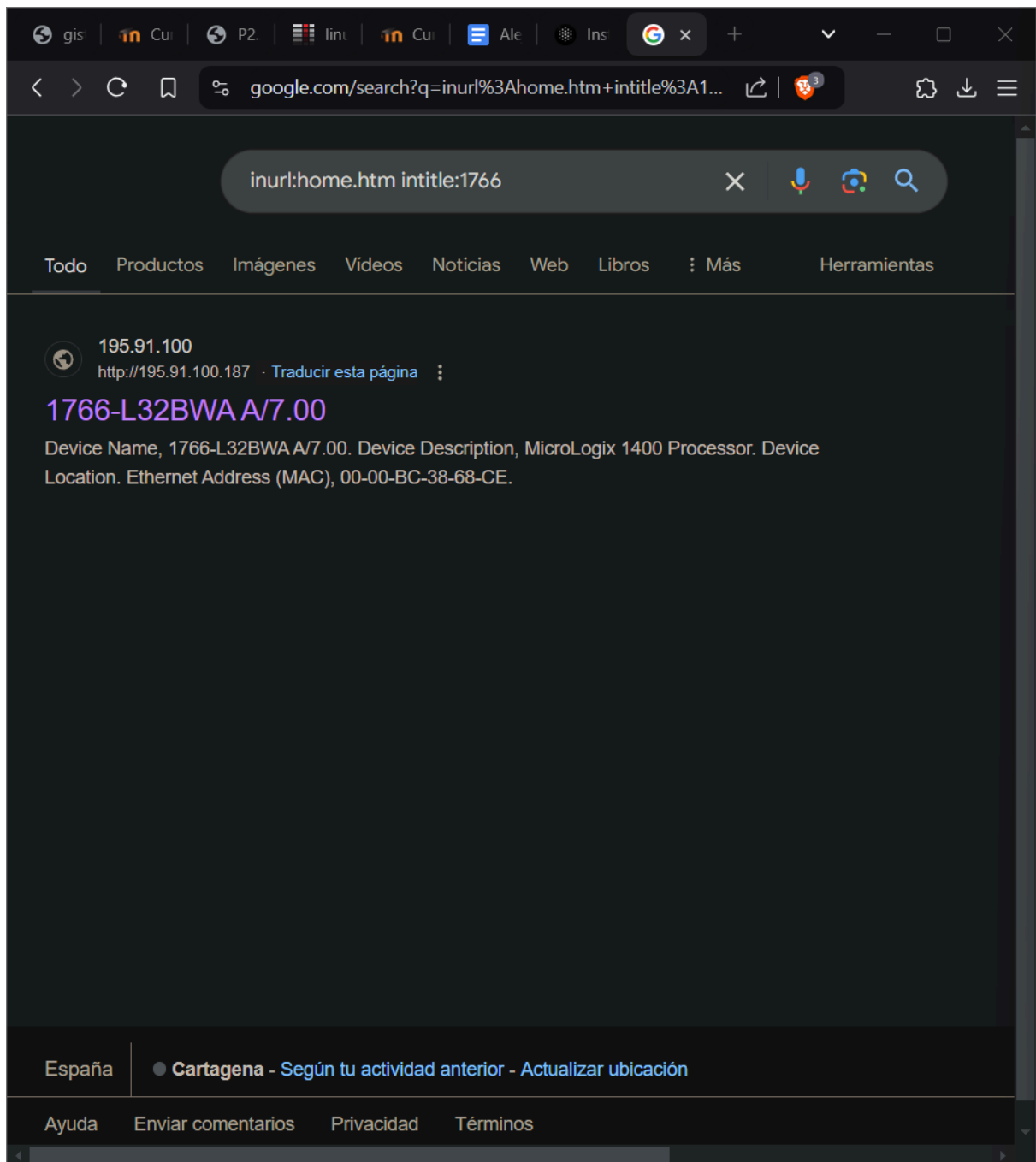
Date Added	Dork
2024-08-23	site:github.com "BEGIN OPENSSSH PRIVATE KEY"
2024-08-23	ext:nix "BEGIN OPENSSSH PRIVATE KEY"
2024-07-26	inurl:home.htm intitle:1766
2024-07-04	intitle:"SSL Network Extender Login" -checkpo
2024-07-04	intext:"siemens" & inurl:"/portal/portal.mwsl"
2024-07-04	Google Dork Submission For GlobalProtect Po
2024-07-04	inurl:"cgi-bin/koha"
2024-07-04	intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json

Google search results for **site:github.com "BEGIN OPENSSSH PRIVATE KEY"**:

- Support OpenSSH private key format for Git SSH ...**  
12 ene 2021 — PEM format keys must be explicitly requested by specifying the "-m PEM" flag.  
→ cat id\_rsa -----BEGIN OPENSSSH PRIVATE KEY----- ...
- OpenSSH keys not accepted · Issue #6312 · rundeck ...**  
24 jul 2020 — -----BEGIN OPENSSSH PRIVATE KEY-----  
b3BlbnNzaC1rZXktZjEAAAAAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAAAAwAAAdzc2gtc...
- Convert SSH private key to classic format**  
If you generate a key pair with ssh-keygen you can, depending on version, get a private key with the header. -----BEGIN OPENSSSH PRIVATE KEY-----.
- Generate private/public key (RSA format)**  
Convert 4096-bit OpenSSH private key to RSA format. # Input -----BEGIN OPENSSSH PRIVATE KEY----- b3BlbnNzaC1rZXktZjEAAAAAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAAAAwAAAdzc2gtc...

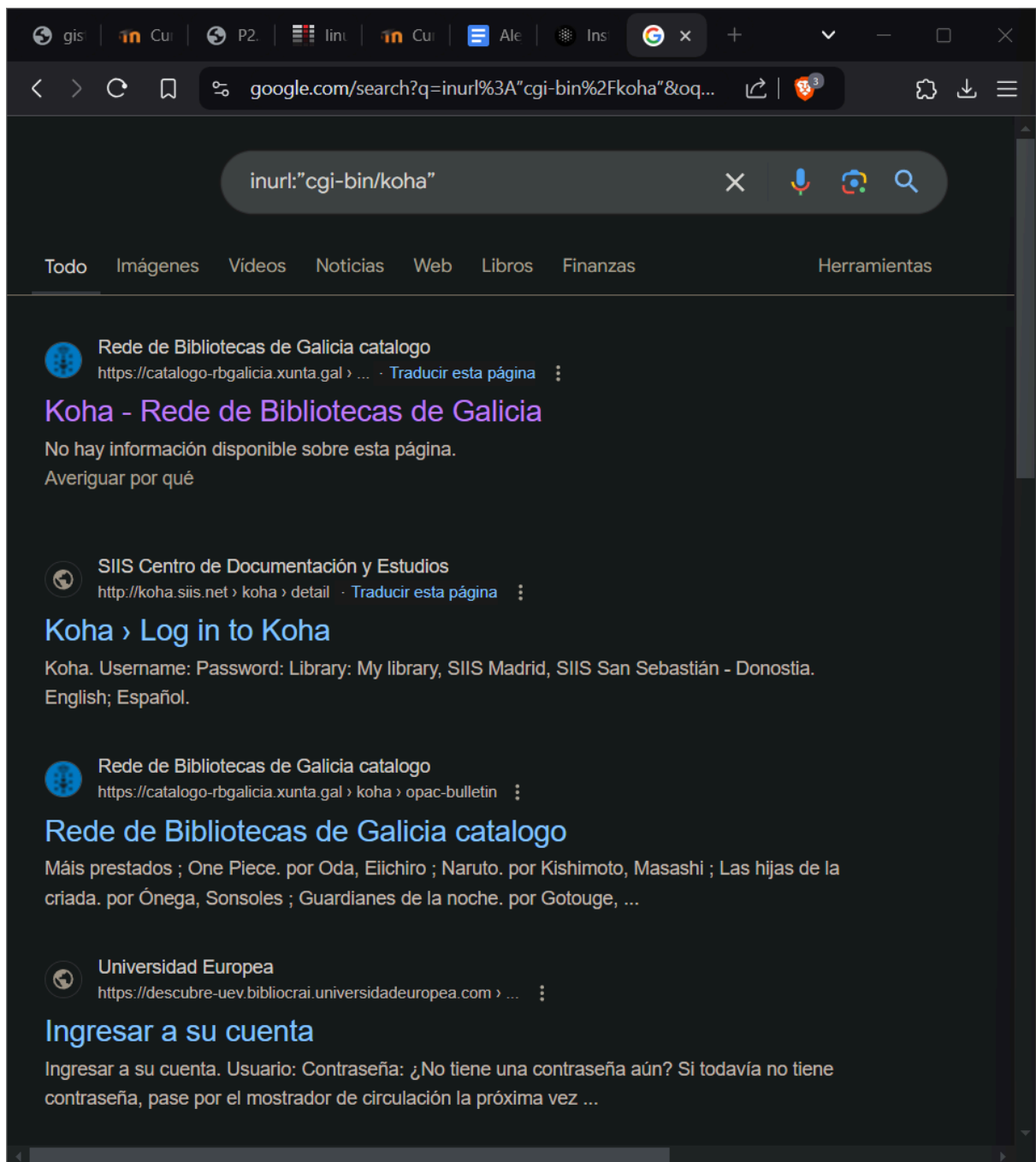
## 2. Dork: **inurl:home.htm intitle:1766**

- Búsqueda: Se encuentra una sola pagina con la informacion de algun dispositivo, la MAC...



### 3. Dork: `inurl:"cgi-bin/koha"`

- Búsqueda: Muestra catálogos de bibliotecas en línea que utilizan koha.





## Parte 2: Exploración de Shodan

### Búsquedas Avanzadas en Shodan

#### 1. Búsqueda: port:80 country:JP

- Resultados: Se encontraron millones de resultados con el puerto 80 abierto en Japón.

The screenshot shows the Shodan search results page for the query 'port:80 country:JP'. The browser address bar shows 'shodan.io/search?query=port%3A80+country%3AJP'. The Shodan logo and search bar are at the top. The search bar contains the query 'port:80 country:JP'. Below the search bar, the 'TOTAL RESULTS' are displayed as '2,595,377'. To the left, there are sections for 'TOP CITIES' and 'TOP ORGANIZATIONS'. The 'TOP CITIES' section lists Tokyo (1,648,265), Osaka (295,495), Asagaya (113,587), Ibaraki (45,934), and Fukuoka (43,837). The 'TOP ORGANIZATIONS' section lists Amazon (576,463), Akamai (249,913), Amazon (246,220), KDDI (138,907), and SAKURA (121,843). The main content area displays search results. The first result is for '218.40.14.52' with a timestamp of '2024-11-15T16:50:24.262934'. It shows the organization 'YAMATO SYSTEM DEVELOPMENT CO., LTD.' and various HTTP headers. The second result is for '401 Authorization Required' with a timestamp of '2024-11-15T16:50:16.897192'. It shows the organization 'KDDI Web Communications Inc.' and various HTTP headers. The third result is for 'Authorization required and not succes...' with a timestamp of '2024-11-15T16:50:15.760492'. It shows the organization 'nginx' and various HTTP headers.

Shodan

port:80 country:JP

TOTAL RESULTS

2,595,377

TOP CITIES

Tokyo 1,648,265

Osaka 295,495

Asag... 113,587

Ibaraki 45,934

Fukuoka 43,837

More...

TOP ORGANIZATIONS

Amaz... 576,463

Akam... 249,913

Amaz... 246,220

KDDI ... 138,907

SAK... 121,843

More...

TOP PRODUCTS

Apac... 683,350

nginx 370,778

View Report

Browse Images

View on Map

Advanced Search

Product Spotlight: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

218.40.14.52

2024-11-15T16:50:24.262934

YAMATO SYSTEM DEVELOPMENT CO., LTD.

Japan, Osaka

HTTP/1.1 200 OK

Date: Fri, 15 Nov 2024 16:45:55 GMT

Server: Apache

X-XSS-Protection: 1; mode=block, 1; mode=block

Content-Security-Policy: reflected-xss block, frame-ancestors 'self'

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

Last-Modified: Wed, 17 Jan 2024 07:43:17 GMT

E...

401 Authorization Required

2024-11-15T16:50:16.897192

150.60.7.185

KDDI Web Communications Inc.

Japan, Asagaya-minami

HTTP/1.1 401 Authorization Required

Date: Fri, 15 Nov 2024 16:50:16 GMT

Server: Apache

WWW-Authenticate: Basic realm="Protected Area"

Vary: Accept-Encoding

Content-Length: 401

Connection: close

Content-Type: text/html; charset=iso-8859-1

Authorization required and not succes...

2024-11-15T16:50:15.760492

220.147.138

HTTP/1.1 401 Authorization Required

## 2. Búsqueda: product:"Apache"

- Resultados: Busca servidores usando Apache, cerca de 15 millones en total.

The screenshot shows the Shodan search interface with the query 'product:Apache'. The total number of results is 14,882,634. The interface includes a sidebar with 'TOP COUNTRIES' and 'TOP PORTS', and a main content area with a detailed view of a specific result.

**TOTAL RESULTS**  
14,882,634

**TOP COUNTRIES**

Country	Count
United States	4,667,360
Japan	1,486,146
Germany	1,462,516
China	704,616
France	675,317

**TOP PORTS**

Port	Count
80	7,151,006
443	5,835,226
8080	416,562
8443	156,348
8081	152,634

**Result Details:**

- IP: 122.28.53.210
- Domain: www.kyushu-toho.co.jp
- Organization: Kyushu Toho Corporation
- Server: Apache
- HTTP/1.1 200 OK
- Date: Fri, 15 Nov 2024 18:00:27 GMT
- X-Powered-By: PHP/8.1.29
- Vary: Accept-Encoding, Cookie
- Cache-Control: max-age=3, must-revalidate
- Content-Length: 99193
- Last-Modified: Fri, 15 Nov 2024 17:48:00 GMT
- Content-Type: text/html; charset=UTF-8

## 3. Búsqueda: webcam country:AU

- Resultados: Este hace una búsqueda de webcams en Australia.

The screenshot shows the Shodan search interface with the query 'webcam country:AU'. The total number of results is 47. The interface includes a sidebar with 'TOP CITIES' and 'TOP PORTS', and a main content area with a detailed view of a specific result.

**TOTAL RESULTS**  
47

**TOP CITIES**

City	Count
Sydney	30
Perth	8
Brisbane	2
Melbourne	2
Goulburn	1

**TOP PORTS**

Port	Count
8081	5
80	3
5000	3
8001	3
8080	3

**Result Details:**

- IP: 172.105.170.119
- Domain: 172.105.170.119
- Organization: Linode
- Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDA
- HTTP/1.1 200 OK
- Date: 2024-11-15T15:44:37.782567

**Result Details:**

- IP: 122.151.144.59
- Domain: 122.151.144.59
- Organization: Vocus Retail
- Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDA
- HTTP/1.1 401 Unauthorized
- Date: 2024-11-15T14:40:07.236941

**Result Details:**

- IP: 172.105.174.178
- Domain: 172.105.174.178
- Organization: Linode
- Server: 360 web server, 792/71644 HTTP Server version 2.0 - TELDA
- HTTP/1.1 200 OK
- Date: 2024-11-15T11:34:31.805459

## Parte 3: Reflexión ética

El uso de herramientas como Google Hacking y Shodan plantea importantes consideraciones éticas y legales.

Uno de los riesgos más significativos de utilizar estas herramientas en sistemas no autorizados es la posibilidad de exponer información sensible, lo que puede resultar en violaciones de datos y daños a la reputación de la organización. Además, la recopilación de información sin permiso puede ser considerada como un acto de intrusión, que podría tener consecuencias legales graves.

En conclusión, aunque Google Hacking y Shodan son herramientas poderosas para la recopilación de información, su uso debe ser guiado por principios éticos y legales.